THE CYCLIC GROUP AS A BASIC ELEMENT IN THE THEORY OF NUMBERS.

By G. A. MILLER, University of Illinois.

The main objects of the present paper are to point out some of the uses of properties of the cyclic group in studying some of the fundamental theorems of number theory, and to develop these properties of the cyclic group by means of elementary arithmetic considerations, which relate mainly to additive number theory. It is hoped that the paper may serve the double purpose of furnishing an easy but rigorous arithmetic introduction to the cyclic group, and of presenting somewhat novel proofs of wide scope for a few very elementary theorems in number theory.

No knowledge of group theory is presupposed, and the only knowledge of number theory that is presupposed is the fact that a rational integer can be resolved into its prime factors in essentially only one way, together with some familiarity with the elementary notions of a congruence* and of a complete system of residues. Hence the substance and the mode of presentation of this paper would appear suitable for a second chapter of an elementary work on number theory. In fact, it presupposes only a very brief first chapter.

§ 1. Order of a Rational Integer (mod m).

The term *order* of a rational integer a with respect to modulus m, m being a positive rational integer, will be used for the smallest positive rational integer b which is such that the product ab is divisible by m. In other words, the order of a (mod m) is equal to the least number of times that a must be taken as an addend in order to obtain a sum that is divisible by m, and hence the order of a is its period (mod m) as regards addition. It is evident that the order of a (mod m) is equivalent to the product of all the prime factors of m which are not also found in a, and hence *all the rational integers which are congruent to the integer* a *(mod* m*) have the same order (mod* m*)*.

The m successive rational integers,

$$1,\ 2,\ 3,\ \ldots,\ m, \qquad (A)$$

which represent the complete system of residues (mod m) composed of the smallest possible natural numbers, must therefore represent also numbers of all the possible orders (mod m). All these orders divide m and there is at least one number in (A) whose order is an arbitrary divisor of m.

* Two rational integers a, b are said to be congruent with respect to modulus m whenever $a-b$ is divisible by the rational integer m. This fact is denoted, according to Gauss, by $a \equiv b \pmod{m}$.

Suppose that $m=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\lambda^{\alpha_\lambda}$; $p_1, p_2, \ldots, p_\lambda$ being distinct rational prime numbers. A necessary and sufficient condition that a is of order $p_\beta^{\alpha_0}$ (mod m), $1 \leqq \beta \leqq \lambda$, is that a is a multiple of $m \div p_\beta^{\alpha_0}$ which is not divisible by $p_\beta^{\alpha_\beta - \alpha_0 + 1}$. There are, therefore, in (A) exactly $p_\beta^{\alpha_\beta}$ numbers whose orders are powers of p_β, viz., the numbers

$$\frac{m}{p_\beta^{\alpha_\beta}}, 2\frac{m}{p_\beta^{\alpha_\beta}}, 3\frac{m}{p_\beta^{\alpha_\beta}}, \ldots, p_\beta^{\alpha_\beta} \frac{m}{p_\beta^{\alpha_\beta}}.$$

We shall use n_β to represent any one of these $p_\beta^{\alpha_\beta}$ numbers, and hence the sum

$$n_1 + n_2 + n_3 + \ldots + n_\lambda \tag{B}$$

may represent any one of m numbers.

It is not difficult to prove that the totality of the possible numbers represented by (B) is a complete system of residues (mod m). To prove this it is only necessary to show that no two of these numbers are congruent (mod m). In fact, from the congruence

$$n_1 + \ldots + n_\beta + \ldots + n_\lambda \equiv n'_1 + \ldots + n'_\beta + \ldots + n'_\lambda \pmod{m}.$$

it results, if $n_0 = n_{\lambda+1} = 0$, that

$$n_1 + \ldots + (n_\beta - n'_\beta) + \ldots + n_\lambda \equiv n'_1 + \ldots + n'_{\beta-1} + n'_{\beta+1} + \ldots + n'_\lambda \pmod{m}.$$

As all these addends, except $n_\beta - n'_\beta$, are divisible by $p_\beta^{\alpha_\beta}$ this number must also divide $n_\beta - n'_\beta$ and hence $n_\beta = n'_\beta$, since all of these numbers may be supposed to be in (A). This proves the following theorem:

If the rational integer m is divisible by exactly λ distinct rational prime numbers, a complete system of residues (mod m) may be obtained by adding successively the numbers of each of the m possible different sets of λ numbers whose orders are powers of the λ different prime factors of m, the numbers having been selected from any complete system of residues (mod m).

To illustrate this theorem we let $m=60=2^2.3.5$. The numbers of (A) whose orders are powers of 2, 3, and 5, respectively, constitute the following rows:

15, 30, 45, 60
20, 40, 60
12, 24, 36, 48, 60

It is not difficult to verify that the 60 different sums obtained by taking one and only one addend from each of these three rows constitutes a complete system of residues (mod 60).

Suppose that p_β^α is the highest power of p which divides the order of a (mod m), and that the order of b (mod m) is not divisible by p_β^α. It results directly from the definition of order that the highest power of p_β which divides a is ${}_\beta^\alpha\beta^{-\alpha}$ and that b is divisible by a higher power of p_β. Hence $a+b$ is divisible by $p_\beta^{\alpha\beta-\alpha}$ but not by the $(\alpha_\beta - \alpha + 1)$th power of p_β, since the latter of these numbers divides b but does not divide a. This proves the theorem:

If p^α is the highest power of a rational prime number which divides the order (mod m) of one of two rational integers without dividing this order of the other, then the order (mod m) of the sum of these integers is divisible by p^α but not by $p^{\alpha+1}$.

From this theorem we can readily deduce the following useful corollary: *If the orders of two or more rational integers are relatively prime, the order of their sum is the product of their orders, all orders being taken with respect to the same modulus.*

The number of the numbers in (A) whose orders are m is denoted by $\phi(m)$ according to Gauss,* and this number is called the *Euler function* of m because Euler first found a general formula for its value. This number has also been called the *indicator* of m by Cauchy, and the *totient* of m by Sylvester. These three terms for the same function of m are still in common use. It is evident that $\phi(m)$ is the total number of the different sets, each set being composed of all congruent numbers (mod m), which involve the numbers of order m (mod m). When $m=p^\alpha$, p being a prime number, it is easy to see that

$$\phi(\mathrm{m})=\phi(p^\alpha)=p^\alpha - p^{\alpha-1}=p^{\alpha-1}(p-1)=p^\alpha(1-1/p),$$

since only $p^{\alpha-1}$ of the numbers of (A) are divisible by p when $m=p^\alpha$, viz., the numbers,

$$p,\ 2p,\ 3p,\ \ldots,\ p^{\alpha-1}.p.$$

From this formula it results that exactly $p_\beta^{\alpha\beta}(1-1/p_\beta)$ of the given n_β numbers in (A) are of order $p_\beta^{\alpha\beta}$, $1 \leqq \beta \leqq \lambda$. The complete system of residues (mod m)

$$n_1+n_2+n_3+\ldots+n_\lambda \qquad \text{(B)}$$

must therefore contain exactly

Disquisitiones Arithmeticae, 1801, Art. 38; German edition, 1889, p. 22.

$$p_1^{\alpha_1}(1-\frac{1}{p_1}).p_2^{\alpha_2}(1-\frac{1}{p_2}).p_3^{\alpha_3}(1-\frac{1}{p_3})\ldots p_\lambda^{\alpha_\lambda}(1-\frac{1}{p_\lambda})$$

$$=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_\lambda})$$

numbers of order m, since the order of the sum of such a set of λ numbers is equal to the product of their orders according to the given theorem, and the choice of one of these λ numbers does not restrict the choice of another. We have therefore established Euler's formula,

$$\phi(m)=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_\lambda}).$$

The number of numbers of order p_β^γ, $0\leqq\gamma\leqq\alpha_\beta$, in n_β is $\phi(p_\beta^\gamma)$ since n_β contains exactly p_β^γ numbers whose orders divide p_β^γ and $1/p_\beta$ of these have orders which divide $p_\beta^{\gamma-1}$. Since all the numbers of (A) whose orders divide d are multiples of m/d it results that (A) contains exactly d numbers whose orders divide d if d is an arbitrary divisor of m. These d numbers include exactly $\phi(d)$ numbers of order d in accord with what was proved above. As all the numbers of (B) have an order which divides m it results from this that

$$m=\phi(d_1)+\phi(d_2)+\ldots+\phi(d_l),$$

where d_1, d_2, ..., d_l are all the positive integral divisors of m, including 1, and m, and hence the second member of this equation gives the sum of the numbers of the integers of the same order in a complete system of residues (mod m).

If $m=m_1m_2$, where m_1, m_2 are relatively prime, we may assume that the orders of numbers in n_1, n_2, ..., n_δ divide m_1, while those in $n_{\delta+1}$, ..., n_λ divide m_2. Hence there are $\phi(m_1)$ numbers of order m_1 in $n_1+n_2+\ldots+n_\delta$ and there are $\phi(m_2)$ numbers of order m_2 in $n_{\delta+1}+\ldots+n_\lambda$. The sum of any one of the former $\phi(m_1)$ numbers and any one of the latter $\phi(m_2)$ numbers is of order m since these orders are relatively prime. Since this sum can be formed in $\phi(m_1).\phi(m_2)$ ways and the number of ways in which this sum can be formed is also $\phi(m)$, it results that $\phi(m)=\phi(m_1)\phi(m_2)$. This formula could also have been deduced directly from Euler's formula,

$$\phi(m)=m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_\lambda}).$$

§ 2. The Cyclic Group of Order m.

If an operation s has the period m it is said to generate the *cyclic group* of order m, and it may be represented by the different powers of s, as follows:

$$s,\ s^2,\ s^3,\ \ldots,\ s^m.$$

The exponents of s form the complete set of residues (mod m) which was denoted by (A) in the preceding section. As the combination* of two or more of these operations is effected by the addition of their exponents (mod m), it results that the abstract properties of the cyclic group are exhibited by the laws governing the addition (mod m) of the numbers in the set

$$1,\ 2,\ \ldots,\ m.$$

From this it follows directly that there is one and only one cyclic group of order m. From the fact that (A) contains exactly $p_\beta^{\alpha\beta}$ numbers whose orders are powers of p_β, it results that the cyclic group of order m contains exactly $p_\beta^{\alpha\beta}$ operators whose orders divide $p_\beta^{\alpha\beta}$. The fact that the numbers

$$n_1+n_2+\ldots+n_\lambda \tag{B}$$

form a complete system of residues is equivalent to the fact that every element or operator or operation of a cyclic group is the product, in one and only one way, of elements whose orders are powers of prime numbers, no two of these orders being powers of the same prime.

The fact that there are exactly d numbers in (A) whose orders divide d, if d is an arbitrary divisor of m, is equivalent to the fact that a cyclic group contains one and only one subgroup whose order is an arbitrary divisor of the order of the group; and the formula

$$m=\phi(d_1)+\phi(d_2)+\ldots+\phi(d_l),$$

where $d_1,\ d_2,\ \ldots,\ d_l$ are all the different divisors of m, including 1 and m, merely asserts that if the numbers of all elements of the various different orders in a cyclic group are added together their sum is the order of this cyclic group.

The fact that $\phi(m)=\phi(m_1)\phi(m_2)$, if $m=m_1m_2$ and $m_1,\ m_2$ are relatively prime, is included in the theorem that a commutative group whose order is divisible by more than one prime is the product of its subgroups of

* This combination is commonly called finding the product of the operations involved.

relatively prime orders, and the order of the product of two commutative elements of a group is equal to the product of the order of these elements whenever these orders are relatively prime. The latter theorem is evidently a special case of the theorem, if the order of one of two commutative elements of a group is divisible by a higher power of a given prime than the order of the other then the order of the product of these two elements is also divisible by this higher power of the given prime, and the highest power of this prime which divides the order of the former element is also the highest power of this prime which divides the order of this product.

These parallel theorems may suffice to exhibit the fact that some of the most fundamental theorems in number theory are also fundamental theorems in group theory, and it seems unfortunate that our elementary books on number theory do not exhibit these points of contact more fully. It should be emphasized that the developments of § 1 are not as simple as they would have been if the properties of the cyclic group had been first developed in the well known manner and if these had been employed in the proof of the given theorems.

The present mode of procedure has been adopted because of the fact that the cyclic group is so fundamental that it seems desirable to establish its fundamental properties in more than one way, and these propertios will doubtless appear more significant if they have been reached by different routes. It may also serve to illustrate relations between additive and multiplicative number theory. In fact, group theory owes a considerable part of its usefulness to the fact that it establishes close contact between additive and multiplicative number theory, as is fully illustrated by the preceding developments.

It may be added that the formula for the $\phi_r(m)$, viz.,

$$\phi_r(m) = m^r\left(1-\frac{1}{p_1{}^r}\right)\left(1-\frac{1}{p_2{}^r}\right)\cdots\left(1-\frac{1}{p^r}\right)$$

results directly from the fact that this formula gives the number of operators of order m in the direct product of r cyclic groups of order m, and hence also in the direct product of $r.\lambda$ cyclic groups of which there are r of each of the orders, $p_1{}^{\alpha_1}$, $p_2{}^{\alpha_2}$, ..., $p_\lambda^{\alpha_\lambda}$. The number of operators of order $p_1{}^{\alpha_1}$ in the direct product of the first r of these subgroups is clearly

$$p_1{}^{\alpha_1 r} - p_1{}^{\alpha_1 r - r} = p_1{}^{\alpha_1 r}(1-1/p_1{}^r),$$

and from this fact the given formula results immediately.*

* Cf. The American Mathematical Monthly, Vol. 11, (1904), p. 129.